Jurnal Teknik Informatika Vol. 17 No. 1, April 2024 (30-39)
ISSN: p-ISSN 1979-9160 (Print)| e-ISSN 2549-7901 (Online)
DOI: https://doi.org/10.15408/jti.v17i1.37256

JURNAL TEKNIK INFORMATIKA

*Homepage* : http://journal.uinjkt.ac.id/index.php/ti

# Systematic Literature Review: Cybersecurity by Utilizing Cryptography Using the Data Encryption Standard (DES) Algorithm

Annisa Desianty[1*] and Imelda Imelda[2]

[1, 2] Faculty of Information Technology, Master of Computer Science, Budi Luhur University
[1, 2] Jl. Ciledug Raya, North Petukangan, District. Pesanggrahan, South Jakarta, 12260, Indonesia

**Article:**
Accepted: March 24, 2024
Revised: December 25, 2023
Issued: April 30, 2024

***Correspondence Address:**
2211601550@student.budiluhur.ac.id

## ABSTRACT

The world of information technology is currently developing very rapidly. This opens up opportunities in the development of computer applications, but it also creates opportunities for threats to alter and steal data or what is often known as cyber-crime. This action is a violation that can cause direct or indirect losses. Therefore, cyber security is very important in protecting user information from cybercrime. Based on this description, this research will conduct a Systematic Literature Review (SLR) on cyber-security by utilizing cryptography using the DES algorithm. By using the SLR method, literature searches were conducted on Google Scholar or Garuda with the keywords for national journals "Data Encryption Standard Algorithm (DES)" and keywords for international journals "Data Encryption Standard Algorithm (DES)" from both national and international journals, and limiting articles from 2019 to 2023, and obtained selection results as many as 10 articles used from national journals and 10 articles used from international journals. This research is expected to increase the understanding of literature that reviews cyber-security by utilizing cryptography using the DES algorithm.

**Keywords :** *Cybersecurity; cryptography; data encryption standard; systematic literature review;*

## 1. INTRODUCTION

The world of information technology is currently developing very rapidly [1]. Information technology always provides convenience for users in services in various fields of life [2]. This opens up opportunities in the development of computer applications, but it also creates opportunities for threats to alter and steal data or what is often known as cybercrime [3].

Cybercrime is a form of crime committed by utilizing computer and internet technology to carry out its crimes [4]. This action is an offense that can cause harm either directly or indirectly [5]. Cyber-crime actions include ransomware attacks, phishing crimes, carding crimes, skimming crimes, OTP fraud, SIM swap, online fraud, data falsification, website and email hacking, plagiarizing other people's websites, illegal context crimes, cyber terrorism, cyber espionage [6]. Therefore, cyber-security is very important in protecting user information from cyber-crime [7]. Many ways are used to secure data, one of which is by utilizing cryptography. Cryptography in cyber-security is important to maintain data confidentiality [8].

Related research has been conducted by Fauzi & Rahayu [9] which discusses digital image security. The problem behind this research is that unauthorized people can steal and access confidential images. So, to overcome these problems, the Data Encryption Standard (DES) algorithm is applied to pixel extraction. The result of this research is the use of DES on bytes "47 117 78 44 118 1 199 20" using the key "KEY123", successfully producing the initial bytes of the Image file, namely "185 94 3 0 255 216 255 224". Another research conducted by Laia, Nugroho, & Halim [10] discusses securing daily production data at PT Cogindo. The problem behind this research is that data or information is very important to maintain confidentiality. So, it is necessary to secure daily production by utilizing cryptography and the DES algorithm. The results of this study carried out an encryption process using an internal key of 64bit to 56bit internal key. Further research was conducted by Pandiangan, Nugroho, & Alhafiz [11] which discusses cryptography to secure employee attendance data at PT Erlangga Mahemeru Publisher Medan. The problem behind this research is the importance of attendance in finding out when employees come, leave the office, or work overtime. It is necessary to secure employee daily attendance data so that unwanted things do not happen. So, encoding is needed to maintain the attendance data using the DES algorithm. The results of this study are successfully implementing cryptography with the help of the Microsoft Visual Studio 2012 programming language, and based on the results of testing, the system is able to perform encryption and decryption on existing attendance data.

Other research conducted by Wayangkau [12] discusses the encryption of sound wave data. The problem behind this research is securing important sounds (audio). So that, data security is needed, namely using the DES algorithm. The result of this research is a successfully built application with a level of sound data security that cannot be accessed by other users because the sound data file has been encrypted. Further research conducted by Dwitri, Sindi, Sihombing, & Gunawan [13] discusses securing document file data. The problem behind this research is the many cases of tapping on information that requires the owner to secure data. So from these problems, information security is needed on data using the DES algorithm. The result of this research is that it can secure the data and the authenticity of the document using the stages in the DES algorithm process.

Other research was also conducted by Simanjuntak, Aspriyono, & Rohmawan [1] which discusses network-based text messaging security. The background of this research is that security is very important in sending confidential text messages. So, an application is needed at PUSKOM Dehasen University Bengkulu to secure these text messages using the DES algorithm. The result of this research is that the application is successfully built, and based on testing, the application can encrypt and decrypt text messages by applying the DES algorithm. Further research has been conducted by Oktami, Nugroho, & Murniyanti [14] which discusses the security of data transactions for truck transportation rental fees at PTPN II. The problem behind this research is that the increasing demand makes the company experience overload, so additional rental truck transportation and increased rental costs are needed. So, from these problems, the company needs a security application to protect the transaction data of truck transportation rental fees by using the DES algorithm. The result of this research is that the application was successfully built and can help secure transaction data for transportation rental fees at the company.

Based on the problems and related research, this research will conduct a Systematic Literature Review (SLR) on cyber-security by utilizing cryptography using the DES algorithm. This is because cryptography is able to maintain information security, such as confidentiality and authentication. At the same time, the DES algorithm is a block cipher algorithm for information security using a symmetric method in encrypting and decrypting data or information [15] so this research is expected to increase the understanding of the literature that reviews cyber-security by utilizing cryptography using the DES algorithm.

## 2. METHODS

This research uses the Systematic Literature Review (SLR) method. SLR aims to identify, review, and interpret all available research with the topic area of the dancing phenomenon and certain relevant research questions [16]. The SLR stages that will be used in this study are the formulation of research questions, literature search, and determination of inclusion and exclusion criteria, but this study did not determine the exclusion criteria because the study did not use articles outside the discussion used in this study, selecting literature, presenting data, processing data and drawing conclusions [17]. The following in Figure 1 are the stages of SLR.

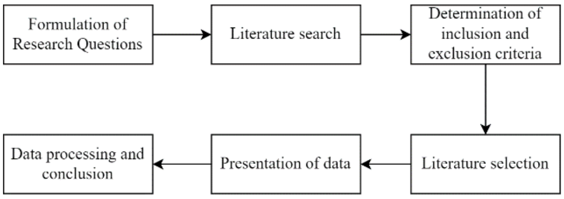

Formulation of Research Questions
Literature search
Determination of inclusion and exclusion criteria
Literature selection
Presentation of data
Data processing and conclusion

**Figure 1.** *SLR stages*

First, the question is how many studies are relevant for cyber-security by utilizing cryptography using DES algorithm. Second, the literature search was conducted on Google Scholar or Garuda with the keywords for national journals "Data Encryption Standard Algorithm (DES)" and keywords for international journals "Data Encryption Standard Algorithm (DES)" from either national or international journals, and limiting articles from 2019 to 2023. Third, the inclusion criteria used in the literature search include studies related to cyber-security using cryptography using the DES algorithm and research results published in journals. Fourth, the literature was obtained, selected, and analyzed based on the inclusion and exclusion criteria, with the selection results of 10 articles from national journals and 10 from international journals. In the next stage, th e articles were listed in a table. Then, an intense review was carried out, especially in the research results section. At the end of the study, a comparison of the findings of several articles was carried out, and made a conclusion.

## 3. RESULTS AND DISCUSSION

### 3.1. Search Result

Table 1 shows the search results from both national and international journals.

**Table 1.** *Grouping by journal*

| No | Journal Type | Total |
|---|---|---|
| 1. | CyberTech Journal | 2 |
| 2. | Zero: Journal of Science, Mathematics, and Applied | 1 |
| 3. | Science and Computer (SAINTIKOM) | 1 |
| 4. | e-Proceeding of Engineering | 1 |
| 5. | ULTIMATICS | 1 |
| 6. | Journal of Computer Science Media | 1 |
| 7. | INSTEK Journal (Informatics Science and Technology) | 1 |
| 8. | Inti Nusa Mandiri | 1 |
| 9. | Journal of Computers, Information, and Technology | 1 |
| 10. | Proceedings of the 2nd International Conference on Information Science and Systems | 1 |
| 11. | Springer Nature Switzerland | 1 |
| 12. | Indonesian Journal of Electrical Engineering and Computer Science | 1 |
| 13. | Journal of Communications | 1 |
| 14. | Hindawi | 1 |
| 15. | International Research Journal of Modernization in Engineering Technology and Science | 1 |
| 16. | International Journal of Scientific Research in Computer Science and Engineering | 1 |
| 17. | Journal of Information Security & Cybercrimes Research | 1 |
| 18. | International Journal of Information Technology | 1 |
| 19. | Turkish Journal of Computer and Mathematics Education | 1 |
| | **Total** | **20** |

## 3.2. Relevant Reference

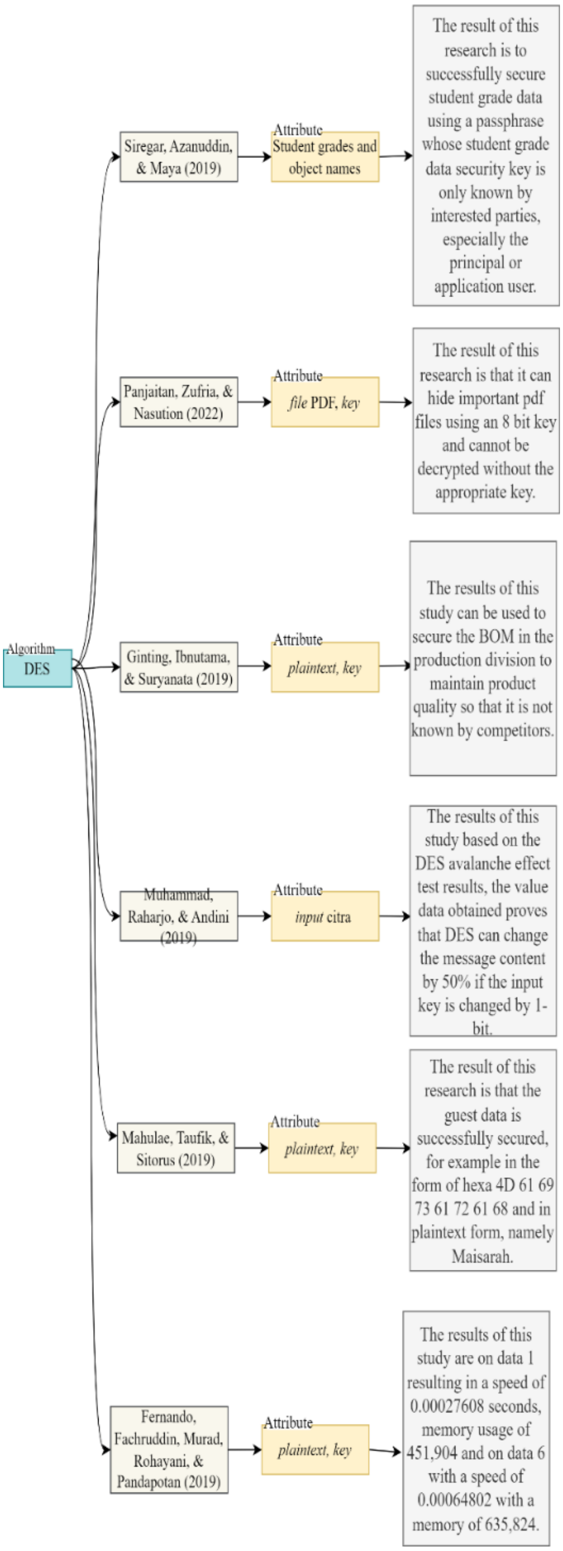
The following in Table II. is a presentation of an overview of the existing literature.

**Table 2.** *Overview of the existing literature*

*Table 2 continued…*

| Author and year | Algorithm | Research Results |
|---|---|---|
| Siregar, Azanuddin, & Maya, 2019 [15] | DES | Successfully secured student grade data and student grades are only known by interested parties |
| Panjaitan, Zufria, & Nasution, 2022 [18] | DES | It can hide important pdf files and cannot be decrypted without the appropriate key. |
| Ginting, Ibnutama, & Suryanata, 2019 [19] | DES | Can be used to secure data on BOM in the Production Division to maintain the quality of a company's products so that they are not known by competitors. |
| Muhammad, Raharjo, & Andini, 2019 [20] | DES | The avalanche effect test results prove that DES can change the message content by 50% if the input key is changed by 1-bit. |
| Mahulae, Taufik, & Sitorus, 2019 [21] | DES | The guest data is secured using a combination of DES cryptography so that it is difficult to find out and read the guest data. |
| Fernando, Fachruddin, Murad, Rohayani, & Pandapotan, 2019 [22] | DES | The test results on data 1 have a speed of 0.00027608 seconds, with a memory usage of 451,904, and on data 6, with a speed of 0.00064802, with memory usage of 635,824. |
| Suwarni, Wahyudi, & Khairil, 2023 [23] | DES, and AES | The result of this research is based on the encryption process time, and it was found that the AES algorithm is faster than the DES algorithm. |
| Altim & Faisal, 2019 [24] | DES, and RC4 | In RC4, a 234,496-byte audio file takes 39.33 seconds. Meanwhile, the DES algorithm for 234,496-byte audio files takes 35.42 seconds. |
| Setiawan, Kamila, & Yulandi, 2022 [25] | DES, ElGamal, 3DES | When the input file is 4KB in size, the ciphertext memory allocation in ElGamal is only 11.9KB, while for DES and 3DES the allocation reaches 32KB. |
| Saputra, Wahyudi, & Jumadi, 2022 [26] | DES, Blowfish | The DES algorithm has a faster time than the Blowfish algorithm with a percentage of the DES algorithm encryption process time of 3.7975%. |
| Amorado, Sison, & Medina, 2019 [27] | DES | Produces an average avalanche effect of 55% due to the vibration of one bit in the plaintext. |
| Akande, Abikoye, Kayode, Aro, & Ogundokun, 2020 [28] | DES | The result of this study was a higher avalanche effect of 90.43% recorded by the traditional DES compared to 87.50% achieved by the modified DES, |
| Kasiran, Ali, & Noor, 2019 [29] | DES, and AES | The AES algorithm performs better in terms of time taken than DES. |
| Alani, Alrammal, & Naveed, 2020 [30] | DES | Experiment with 2000 IoT devices successfully found the key in 0.015 seconds |
| Lu, 2022 [31] | DES | The results of this study show that the sensitivity value is between 5 and 6.6. |
| Reddy, et al., 2020 [32] | DES | This research results show that the total time required for encryption reaches 42.15 seconds when used with two systems. |
| Logunleko, Adeniji, & Logunleko, 2020 [33] | DES, AES, EB64 | This research results for plaintext SMS shows that EB64 encryption and decryption time is shorter than AES and DES. |
| Al-gohany & Almotairi, 2019 [34] | DES, AES | This research results that AES is faster than DES in encryption time, but in decryption, DES is faster than AES from 20KB to 100 KB. |
| Patel, 2019 [35] | DES, AES, Blowfish | Experimental results show that Blow fish is a better choice than AES and DES based on the memory used, which takes 1.01% of the time. |
| Soni & Malik, 2021 [36] | AES, AES-Twofish, AES-Blowfish, Twofish-AES, Blowfish-AES, AES-Serpent, Serpent-Twofish, while the 3-tier model is AES, DES-Blowfish-AES, AES-Twofish-Serpent, Serpent-Twofish-AES. | The results are the best model obtained by hybrid AES-Twofish, Serpent-Twofish, and hybrid AES-Blowfish. The AES-Blowfish hybrid provides the highest security and avalanche effect, ranging from 49.5-53.65%. |

Figures 2, 3, and 4 are the results of research on cybersecurity by utilizing cryptography using the DES algorithm.


Algorithm
DES
Siregar, Azanuddin, & Maya (2019)
Attribute
Student grades and object names
Panjaitan, Zufria, & Nasution (2022)
Attribute
file PDF, key
Ginting, Ibnutama, & Suryanata (2019)
Attribute
plaintext, key
Muhammad, Raharjo, & Andini (2019)
Attribute
input citra
Mahulae, Taufik, & Sitorus (2019)
Attribute
plaintext, key
Fernando, Fachruddin, Murad, Rohayani, & Pandapotan (2019)
Attribute
plaintext, key

The result of this research is to successfully secure student grade data using a passphrase whose student grade data security key is only known by interested parties, especially the principal or application user.

The result of this research is that it can hide important pdf files using an 8 bit key and cannot be decrypted without the appropriate key.

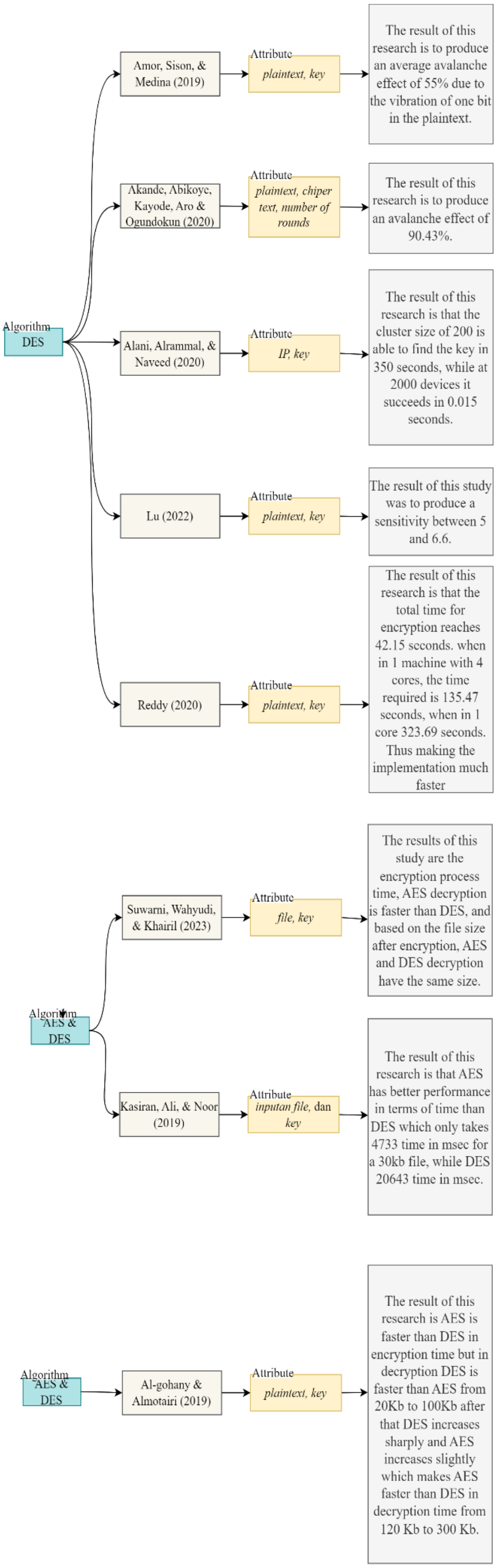
The results of this study can be used to secure the BOM in the production division to maintain product quality so that it is not known by competitors.

The results of this study based on the DES avalanche effect test results, the value data obtained proves that DES can change the message content by 50% if the input key is changed by 1-bit.

The result of this research is that the guest data is successfully secured, for example in the form of hexa 4D 61 69 73 61 72 61 68 and in plaintext form, namely Maisarah.

The results of this study are on data 1 resulting in a speed of 0.00027608 seconds, memory usage of 451,904 and on data 6 with a speed of 0.00064802 with a memory of 635,824.

**Figure 2.** *Mapping cyber-security using cryptographic algorithms*


Algorithm
DES
Amor, Sison, & Medina (2019)
Attribute
plaintext, key
Akande, Abikoye, Kayode, Aro & Ogundokun (2020)
Attribute
plaintext, chiper text, number of rounds
Alani, Alrammal, & Naveed (2020)
Attribute
IP, key
Lu (2022)
Attribute
plaintext, key
Reddy (2020)
Attribute
plaintext, key
Algorithm
AES & DES
Suwarni, Wahyudi, & Khairil (2023)
Attribute
file, key
Kasiran, Ali, & Noor (2019)
Attribute
inputan file, dan key
Algorithm
AES & DES
Al-gohany & Almotairi (2019)
Attribute
plaintext, key

The result of this research is to produce an average avalanche effect of 55% due to the vibration of one bit in the plaintext.

The result of this research is to produce an avalanche effect of 90.43%.

The result of this research is that the cluster size of 200 is able to find the key in 350 seconds, while at 2000 devices it succeeds in 0.015 seconds.

The result of this study was to produce a sensitivity between 5 and 6.6.

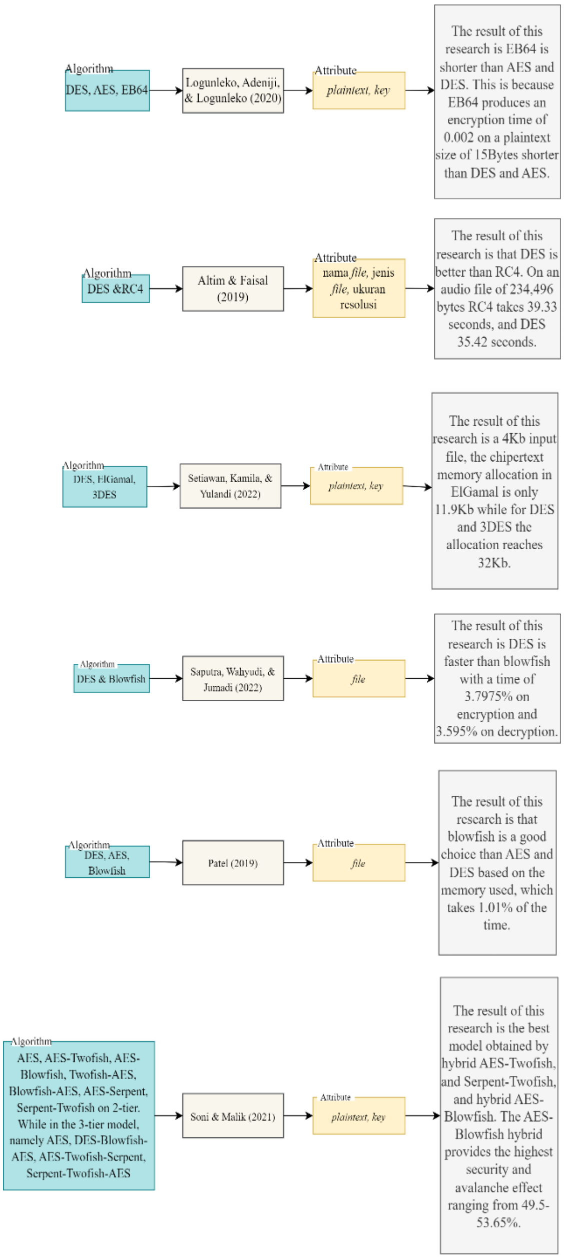
The result of this research is that the total time for encryption reaches 42.15 seconds. when in 1 machine with 4 cores, the time required is 135.47 seconds, when in 1 core 323.69 seconds. Thus making the implementation much faster

The results of this study are the encryption process time, AES decryption is faster than DES, and based on the file size after encryption, AES and DES decryption have the same size.

The result of this research is that AES has better performance in terms of time than DES which only takes 4733 time in msec for a 30kb file, while DES 20643 time in msec.

The result of this research is AES is faster than DES in encryption time but in decryption DES is faster than AES from 20Kb to 100Kb after that DES increases sharply and AES increases slightly which makes AES faster than DES in decryption time from 120 Kb to 300 Kb.

**Figure 3.** *Mapping cyber-security using cryptographic algorithms (continued)*



The result of this research is EB64 is shorter than AES and DES. This is because EB64 produces an encryption time of 0.002 on a plaintext size of 15Bytes shorter than DES and AES.

The result of this research is that DES is better than RC4. On an audio file of 234,496 bytes RC4 takes 39.33 seconds, and DES 35.42 seconds.

The result of this research is a 4Kb input file, the chipertext memory allocation in ElGamal is only 11.9Kb while for DES and 3DES the allocation reaches 32Kb.

The result of this research is DES is faster than blowfish with a time of 3.7975% on encryption and 3.595% on decryption.

The result of this research is that blowfish is a good choice than AES and DES based on the memory used, which takes 1.01% of the time.

AES, AES-Twofish, AES-Blowfish, Twofish-AES, Blowfish-AES, AES-Serpent, Serpent-Twofish on 2-tier. While in the 3-tier model, namely AES, DES-Blowfish-AES, AES-Twofish-Serpent, Serpent-Twofish-AES

The result of this research is the best model obtained by hybrid AES-Twofish, and Serpent-Twofish, and hybrid AES-Blowfish. The AES-Blowfish hybrid provides the highest security and avalanche effect ranging from 49.5-53.65%.

**Figure 4.** *Mapping cyber-security using cryptographic algorithms (continued)*

From Figure 2, Figure 3, and Figure 4 which is a cyber-security mapping conducted by (Siregar, Azanuddin, & Maya, 2019) [15], (Panjaitan, Zufria, & Nasution, 2022) [18], (Ginting, Ibnutama, & Suryanata, 2019) [19], (Muhammad, Raharjo, & Andini, 2019) [20], (Mahulae, Taufik, & Sitorus, 2019) [21], (Fernando, Fachruddin, Murad, Rohayani, & Pandapotan, 2019) [22], (Suwarni, Wahyudi, & Khairil, 2023) [23], (Altim & Faisal, 2019) [24], (Setiawan, Kamila, & Yulandi, 2022) [25], (Saputra, Wahyudi, & Jumadi, 2022) [26], (Amorado, Sison, & Medina, 2019) [27], (Akande, Abikoye, Kayode, Aro, & Ogundokun, 2020) [28], (Kasiran, Ali, & Noor, 2019) [29], (Alani, Alrammal, & Naveed, 2020) [30], (Lu, 2022) [31], (Reddy, et al., 2020) [32], (Logunleko, Adeniji, & Logunleko, 2020) [33], (Al-gohany & Almotairi, 2019) [34], (Patel, 2019) [35], (Soni & Malik, 2021) [36]. These studies use different algorithms. Apart from using the DES algorithm, some studies use AES, Blowfish, EB64, RC4, ElGamal, 3DES. In the process, it has attributes such as plaintext, and key. The existing research shows various results, such as using the avalance effect, the total time required to perform the process, and the sensitivity and memory used.

## 3.3. Analysis and Discussion

Data security on a network, application, computer, system, text, and so on is very important for its owner to prevent unwanted things from happening. Such as ransomware attacks, phishing crimes, carding crimes, skimming crimes, OTP fraud, SIM swap, online fraud, data falsification, website and email hacking, plagiarizing other people's websites, illegal context crimes, cyber terrorism, cyber espionage. By utilizing cryptography using can maintain information security in the form of confidentiality, data integrity, and data validity, and it can be used to ensure that information is not manipulated or inform the authenticity of information or user identity.

From the results of the literature review, all algorithms have their own uniqueness with different applications and have their own advantages and disadvantages. Several applications are using DES that can work in existing applications, both to secure student grades [15], hide PDF files [18], secure data in companies [19], change messages by 50% [20], able to secure guest data [21], able to be implemented on IoT devices [22], able to secure exhaustive attacks and cryptanalysis attacks [27], can produce high avalanche effect [28], can be applied to IoT [30], can secure accounting data with sensitivity between 5 and 6. 6 [31] [32]. In addition, some applications show that AES is a faster algorithm than DES [23] [29]. In another study, EB64 has a shorter encryption and decryption time to secure SMS than DES and AES [33]. In another study, which compared DES and AES showed that both have their own advantages, where AES is faster in the encryption process and DES is faster in the data decryption process [34].

Another study shows that DES is better than RC4 because it only takes 35.42 times faster than RC4 [24]. Other algorithms used as a comparison are ElGamal, DES, 3DES, which results in ElGamal having better performance in memory storage than DES, 3DES [25]. Blowfish shows better results based on memory used than AES and DES [35]. But on the other hand, DES has a better percentage of encryption time than Blowfish [26]. While the results of the hybrid process obtained AES-Twofish is a good model when applied [36].

From the existing literature, the application of comparison or combination is very important to produce good results. However, the comparison or combination can be considered from the security needs and application of the system to be used. If the comparison can be suggested for the selection of cryptographic algorithms that have been recommended and have good results from existing research. Whereas the use of a combination can be for stronger resistance to existing attacks, and if one algorithm is found to be vulnerable, it can be used as a combination.

In addition, based on the review of several related journals, the stages of DES implementation can be seen in Figure 2 [37].

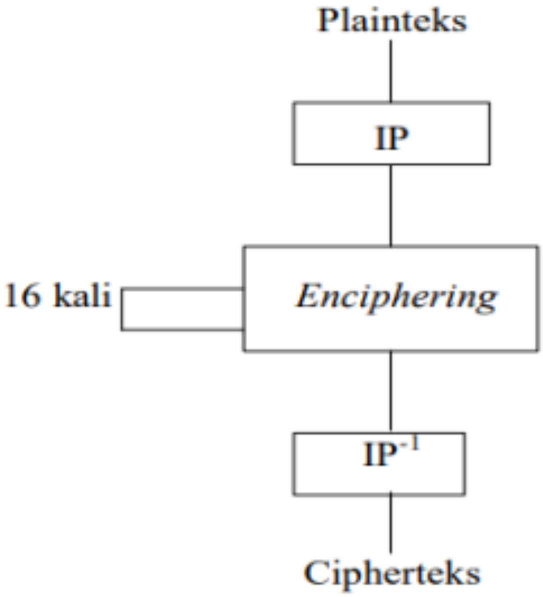


**Figure 5.** *Skema DES*

From Figure 5 the plaintext block is permuted with the initial permutation matrix (IP). Then the initial permutation result is enciphered 16 times (16 rounds). Each round uses a different internal key. The enciphering result is then mutated with the inverse initial permutation matrix (IP-1) into a ciphertext block.

In general, the DES scheme has two input functions, namely the plaintext to be encrypted with a length of 64 bits, and the key with a length of 56 bits.

In detail, there are three plaintext IPs, namely, (1) the 64-bit plaintext is processed in the IP and reorder the bits to produce input permutations. (2) a step to perform a word loop of a plaintext of 16 by performing a substitution permutation function, in which the final output contains 64 bits (a function of the plaintext and key), enters the swap, and generates a preoutput. (3) The preoutput is processed, and the permutation is inverted from IP, which produces a 62-bit chipertext.

The process of the 56-bit key is (1) the key passes through the function of permutation, (2) shifting the key to select the key permutation loop 16 times, which produces a subkey that is processed with a combination of permutations, (3) the difference from the subkey will be carried out by shifting the key which results in a combination of 64-bit plaintext with a 56-bit key.

In the DES algorithm, encryption and decryption processes [38]. The encryption process includes key expansion. In this process, the secret key, which is initially 56-bit in size, will be converted into a form suitable for use in the DES algorithm, which involves forming a key with a length of 64 bits, with an additional 8-bit function divided into data blocks of a fixed size, each block will be transposed using IP. In the decryption process, the first process, namely key expansion, is used to form a sub-key that will be used in the decryption round. The second is data separation and initial permutation. The encrypted data to be decrypted will be divided into data blocks of 64-bit size, which will be changed using IP and then arranged based on the permutation table. The third is the rounds process, which involves 16 rounds of decryption, similar to the encryption rounds but using subkeys in reverse order. Fourth, the exchange and unification of blocks and the last stage of the final permutation, from the 64-bit data block that has been unified, will go through the final permutation (FP) to rearrange the data bits according to the permutation table.

## 4. FUTURE RESEARCH

Future research is the process of identifying research that can be done in the future, such as questions that have not been answered in current research [39]. This research has presented a literature review on cybersecurity by utilizing cryptography using DES algorithm and comparison with other algorithms such as Advanced Encryption Standard (AES), Blowfish, Twofish, Serpent, EB64, RC4, ElGamal, 3DES. When looking at the application in comparison and the hybrid process in the algorithms used, it can be seen that AES has a larger key length than DES, which can ensure high security. This algorithm is also quite strong in some applications when using Blowfish, but AES is considered more secure from attacks. Meanwhile, when viewed from the application of Twofish, it can be considered quite secure, but Twofish is still not widely applied in various security standards. So, for future research, it is recommended to use AES or a hybrid AES using Twofish or a hybrid AES using blowfish.

## CONCLUSION

Based on the systematic literature review of 10 national and 10 international journals in cyber-security by utilizing cryptography, it can be concluded that the application of cryptography using several algorithms that have been described can be used to encrypt data for data security.

## REFERENCES

[1] H. A. Simanjuntak, H. Aspriyono and E. P. Rohmawan, "Sistem Keamanan Pesan Teks Berbasis Jaringan Menggunakan Algoritma Data Encryption Standard (DES)," *Jurnal Komputer, Informasi dan Teknologi,* pp. 613-621, 2022.

[2] A. B. S. Damanik, I. Gunawan, B. E. Damanik, Sumarno and D. Hartam, "Implementasi Algoritma Data Encryption Standart (DES) Dalam Pengamanan Data Karyawan Ramayana Department Store," *Journal of Computer System and Informatics (JoSYC),* vol. 2, pp. 70-76, 2020.

[3] A. Fauzi, "ANALISA KOMBINASI PESAN TEKS KE DALAM FILE AUDIO MEMANFAATKAN ALGORITMA DATA ENCRYPTION STANDARD DAN METODE END OF FILE," *Jurnal Teknik Informatika Kaputama (JTIK),* pp. 1-8, 2019.

[4] M. A. Suharto and M. N. Apriyani, "Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional," *Risalah Hukum,* vol. 17, pp. 98-107, 2021.

[5] C. Hidayatullah, "Jenis dan Dampak Cyber Crime," *Prosiding SAINTEK: Sains dan Teknologi,* pp. 216-221, 2023.

[6] A. Farid, "13 Contoh Cyber Crime Atau Kejahatan Dunia Maya Yang Berbahaya," 30 Oktober 2022. [Online]. Available: https://www.exabytes.co.id/blog/contoh-cyber-crime/.

[7] D. Nurfadlillah, "ANALISIS SENTIMEN MENGENAI KESADARAN MASYARAKAT INDONESIA TERHADAP KEAMANAN SIBER DALAM MENGHADAPI KEBOCORAN DATA MENGGUNAKAN ALGORITMA NAÏVE BAYES CLASSIFIER," *Jurnal Elektro Luceat,* vol. 9, 2023.

[8] B. Fachri and R. M. Sembiring, "Pengamanan Data Teks Menggunakan Algoritma DES Berbasis Android," *JURNAL MEDIA INFORMATIKA BUDIDARMA,* pp. 110-116, 2020.

[9] A. Fauzi and R. P. Rahayu, "KEAMANAN CITRA DIGITAL DENGAN MEMANFAATKAN PROSES PENERAPAN ALGORITMA DATA ENCRYPTION STANDART (DES) PADA EKTRAKSI PIXEL," *Jurnal Informatika Kaputama(JIK),* vol. 4, pp. 269-279, 2020.

[10] B. N. Laia, N. B. Nugroho and J. Halim, "Implementasi Kriptografi Untuk Pengamanan Data Produksi Harian Dengan Algoritma Data Encryption Standard (DES) Pada PT. Cogindo," *Jurnal CyberTech,* 2020.

[11] A. A. Pandiangan, N. B. Nugroho and A. Alhafiz, "IMPLEMENTASI KRIPTOGRAFI UNTUK MENGAMANKAN DATA ABSENSI KARYAWAN PADA PT. PENERBIT ERLANGGA MAHEMERU MEDAN MENGGUNAKAN (DATA

ENCRYPTION STANDARD )," *Jurnal CyberTech,* pp. 1-15, 2021.

[12] I. H. Wayangkau, "ENKRIPSI DATA GELOMBANG SUARA DENGAN ALGORITMA DES," *MUSTEK ANIM HA,* vol. 10, pp. 60-64, 2021.

[13] N. Dwitri, S. Sindi, I. A. Sihombing and I. Gunawan, "PENGAMANAN DATA FILE DOCUMENT MENGUNAKAN KRIPTOGRAFI ENCRYPTION SYSTEM (DES)," *JISICOM (Journal of Information System, Informatics and Computing),* pp. 40-46, 2020.

[14] D. Oktami, N. B. Nugroho and S. Murniyanti, "Implementasi Kriptografi Keamanan Data Transaksi Biaya Sewa Angkutan Truk Di PTPN II Dengan Mennggunakan Metode DES ( Data Encryption Standard)," *Sains dan Komputer (SAINTIKOM),* pp. 1-15, 2020.

[15] N. D. P. Siregar, Azanuddin and W. R. Maya, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA NILAI SISWA PADA SD NEGERI 064979 MEDAN DENGAN MENGGUNAKAN ALGORITMA DES," *Jurnal CyberTech,* 2019.

[16] F. Triandini, S. Jayanatha, A. Indrawan, G. W. Putra and B. Iswara, "Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia," *Indonesian Journal of Information Systems (IJIS),* pp. 63-78, 2019.

[17] D. Fitriani and A. Putra, "Systematic Literature Review (SLR):Eksplorasi Etnomatematika pada Makanan Tradisional," *Journal of Mathematics Education and Learning,* pp. 18-27, 2022.

[18] A. W. Panjaitan, I. Zufria and Y. R. Nasution, "Implementation of Data Encryption Standard (DES) Algorithm for Data Security on PDF Documents," *Zero : Jurnal Sains, Matematika, dan Terapan,* pp. 231-237, 2022.

[19] E. F. Ginting, K. Ibnutama and G. Suryanata, "Implementasi DES (Data Encryption Standard) Untuk Penyandian Data Bill Of Material pada Divisi Produksi PT.Siantar Top, Tbk," *Sains dan Komputer (SAINTIKOM),* pp. 161-166, 2019.

[20] R. Muhammad, J. Raharjo and N. Andini, "IMPLEMENTASI DATA ENCRYPTION STANDARD (DES) PADA IMAGE WATERMARKING CITRA MENGGUNAKAN ALGORITMA DISCRETE COSINE TRANSFORM (DCT)," *e-Proceeding of Engineering,* pp. 4032-4036, 2019.

[21] K. M. Mahulae, F. Taufik and U. F. S. Sitorus, "Implemantasi Kriptografi Pengamanan Data Tamu Pada Hotel Sibayak Multi Menggunakan Metode Data Encryption Standard (DES)," *Jurnal CyberTech,* pp. 1-14, 2019.

[22] E. Fernando, Fachruddin, D. F. Murad, H. Rohayani and Pandapotan, "Analisa Dan Implementasi Algoritma Enkripsi Simetris Data Encryption Standard (DES) Pada Raspberry Pi," *ULTIMATICS,* pp. 55-60, 2019.

[23] M. Suwarni, J. Wahyudi and Khairil, "Comparison of the DES Cryptographic Algorithm and the AES Algorithm in Securing Document Files," *Jurnal Media Computer Science,* vol. 2, pp. 41-48, 2023.

[24] M. Z. Altim and Faisal, "ANALISIS PERBANDINGAN ALGORITMA RIVEST CHIPER 4 (RC4) DAN DATA ENCRYPTION STANDARD (DES) PADA STEGANOGRAFI," *Jurnal INSTEK (Informatika Sains dan Teknologi),* vol. 4, pp. 121-130, 2019.

[25] H. Setiawan, M. I. Kamila and Yulandi, "ANALISIS KECEPATAN ENKRIPSI DEKRIPSI DAN ALOKASI MEMORI MENGGUNAKAN ALGORITMA DES, 3DES DAN ELGAMAL," *INTI NUSA MANDIRI,* vol. 17, pp. 70-78, 2022.

[26] R. P. Saputra, J. Wahyudi and J. Jumadi, "Comparative Analysis of the Blowfish Algorithm and the Des Algorithm in the Document File Encryption and Decryption Process," *Jurnal Komputer, Informasi, dan Teknologi,* vol. 2, pp. 605-612, 2022.

[27] R. V. Amorado, A. M. Sison and R. P. Medina, "Enhanced data encryption standard (DES) algorithm based on filtering and striding techniques," *Proceedings of the 2nd International Conference on Information Science and Systems,* pp. 252-256, 2019.

[28] O. N. Akande, O. C. Abikoye, A. A. Kayode, O. T. Aro and O. R. Ogundokun, "A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security," *Springer Nature Switzerland,* pp. 487-499, 2020.

[29] Z. Kasiran, H. F. Ali and N. M. Noor, "Time performance analysis of advanced encryption standard and data encryption standard in data security transaction," *Indonesian Journal of Electrical Engineering and Computer Science,* pp. 988-994, 2019.

[30] M. M. Alani, M. Alrammal and M. Naveed, "Implementing IoT Lottery on Data Encryption Standard," *Journal of Communications,* vol. 15, pp. 735-741, 2020.

[31] Z. Lu, "Encryption Management of Accounting Data Based on DES Algorithm of Wireless Sensor Network," *Hindawi,* pp. 1-14, 2022.

[32] K. S. Reddy, P. S. Karun, M. C. Shekar, G. S. Charan, P. S. Pavan and M. K, "DISTRIBUTED AND PARALLELIZED IMAGE ENCRYPTION USING DES," *International Research Journal of Modernization in Engineering Technology and Science ,* pp. 280-287, 2020.

[33] Logunleko, Adeniji and Logunleko, "A Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security," *International Journal of Scientific Research in Computer Science and Engineering,* pp. 45-51, 2020.

[34] N. A. Al-gohany and S. Almotairi, "Comparative Study of Database Security In Cloud Computing Using AES," *Journal of Information Security & Cybercrimes Research,* vol. 2, pp. 102-109, 2019.

[35] K. Patel, "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files," *International Journal of Information Technology,* pp. 813-819, 2019.

[36] P. Soni and R. Malik, "Performance Analysis of Cascaded Hybrid Symmetric Encryption Models," *Turkish Journal of Computer and Mathematics Education,* vol. 12, pp. 1699-1708, 2021.

[37] J. H. Sinaga, M. Pangaribuan, Fazly, I. Rivaldo and I. Gunawan, "Penerapan EnkripsiDan DeskripsiMenggunakan Algoritma Data Encryption Standart (DES)Dengan Pemograman Matlab," *JURNAL MEDIA INFORMATIKA[JUMIN],* pp. 63-69, 2022.

[38] A. Pratama, M. N. Arif, M. Nazir, Z. Dannaun and Dara, "ALGORITMA DES ( DATA ENCRYPTION STANDARD ) UNTUK KEAMANAN DIGITAL," *JURNAL SITEBA,* pp. 15-19, 2023.

[39] K. Gondlach, "WHAT IS FUTURES RESEARCH?," 2023. [Online]. Available: https://www.kaigondlach.de/en/what-is-futures-research/.

[40] M. Suwarni, J. Wahyudi and Khairil, "Comparison of the DES Cryptographic Algorithm and the AES Algorithm in Securing Document Files," *Jurnal Media Computer Science,* vol. 2, pp. 41-48, 2023.